UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/881,147	06/14/2001	Geoffrey Cooper	SECU0001CIP	9105

22862 7590 05/09/2006

GLENN PATENT GROUP
3475 EDISON WAY, SUITE L
MENLO PARK, CA 94025

EXAMINER	
KIM, JUNG W	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 05/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/881,147	**Applicant(s)** COOPER ET AL.	
	Examiner Jung W. Kim	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 September 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-16 and 18-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-16 and 18-40* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This Office action is in response to the RCE filed on September 19, 2005.

2. Claims 1-4, 6-16 and 18-40 are pending.

3. Claims 1, 2, 13, 14, 25 and 33 are amended.

4. Claims 5 and 17 are canceled.

Continued Examination Under 37 CFR 1.114

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on September 19, 2005 has been entered.

Response to Arguments

6. Applicant's arguments with respect to amended claims 1-4, 6-16 and 18-40 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

7. Claims 25-40 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim.

Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Dependent claim 25 claims the policy monitor component of claim 13; however, this dependency does not include all limitations of parent claim 13. Similarly, dependent claim 33 claims the policy monitor component of claim 1, but does not claim the remaining features of claim 1. A dependent claim must incorporate every limitation of the claim to which it refers (35 USC 112, 4th paragraph).

Claim Rejections - 35 USC § 112

8. Claims 2 and 14 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

9. Claims 2 and 14 recite the limitation "said synthesized information." There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

10. Claims 1-4, 6, 8-16, 18 and 20-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. USPN 6,499,107 (hereinafter Gleichauf) in view of Rogers et al. U.S. Patent No. 5,557,747 (hereinafter Rogers).

11. As per claim 1, Gleichauf discloses a system for analyzing network traffic to use in performing network and security assessments by listening on a subject network, interpreting events, and taking action, comprising:

a. a policy specification (col. 5:7-15);

b. a network monitor processor that processes network packet data collected from the subject network (5:59-61); and

c. a policy-monitoring component that receives and processes the processed network packet data to assign policy dispositions to network events contained in the network packet data (fig. 2, reference no. 20);

d. wherein the policy monitoring component further comprises a policy engine that:

i. as each network packet arrives, compares the network packet data against the policy specification file and responsive to the comparison assigns associated policy dispositions and level of severity to the network events contained in the network packet data (figs. 5A, 5B and 5C; 4:27-42; 7:63-8:46);

ii. interprets each protocol event (5:63-6:8); and

iii. consults the policy specification file as each protocol event is interpreted to ensure that an earliest determination of the disposition is reached. (9:35-50)

Gleichauf does not expressly disclose that the policy specification is on a file. However, rule based policies are typically listed on a file in the art. As an example, a policy server taught by Rogers, implements a rule-based policy file to define policies. A policy file is scanned in and parsed to build a database, which manages policy updates in response to state changes (col. 2:24-49; Figure 3, Reference No. 24). It would be obvious to one of ordinary skill in the art at the time the invention was made to implement the policy specification as a file since do so enables the policies to be implemented using a conventional format in the art for instantaneous implementation into a computer system and simultaneously being user legible as known to one of ordinary skill in the art. The aforementioned covers the limitations of claim 1.

12. As per claim 2, the rejection of claim 1 under 35 USC 103(a) as being unpatentable over Gleichauf in view of Rogers is incorporated herein. In addition, the policy-monitoring component further comprises:

e. a parser for parsing the policy specification file (Rogers, Figure 3, Reference No. 50); and

f. a logger for logging and storing into an events database the synthesized information by the policy engine according to a logging policy file (Gleichauf, fig. 2, reference no. 36; figs. 5A-C; col. 7:22-27 and lines 57-62; 8:1-8).

13. As per claim 3, the rejection of claim 2 under 35 USC 103(a) as being unpatentable over Gleichauf in view of Rogers is incorporated herein. In addition, the system further comprises a query mechanism for mining the stored data in the events database (Gleichauf, col. 8:20-21).

14. As per claim 4, the rejection of claim 2 under 35 USC 103(a) as being unpatentable over Gleichauf in view of Rogers is incorporated herein. In addition, the system further comprises an alarm script component for generating alarms based on the level of severity of the network events (Gleichauf, col. 8:35-46).

15. As per claim 6, the rejection of claim 1 under 35 USC 103(a) as being unpatentable over Gleichauf in view of Rogers is incorporated herein. In addition, the collected network packet data is captured in a file or is streams-based (Gleichauf, col. 7:63-67).

16. As per claim 8, the rejection of claim 1 under 35 USC 103(a) as being anticipated unpatentable over in view of Rogers is incorporated herein. In addition, the system further comprises a parser for generating an English description policy representation from the policy specification file (Rogers, Figure 3).

17. As per claim 9, the rejection of claim 1 under 35 USC 103(a) as being anticipated unpatentable over in view of Rogers is incorporated herein. In addition the network monitor processor is used in standalone mode (Gleichauf, col. 4:27-34).

18. As per claim 10, the rejection of claim 1 under 35 USC 103(a) as being unpatentable over Gleichauf in view of Rogers is incorporated herein. In addition, the

network monitor processor and the policy-monitoring component run on a same machine (Gleichauf, col. 4:27-34).

19. As per claim 11, the rejection of claim 1 under 35 USC 103(a) as being unpatentable over Gleichauf in view of Rogers is incorporated herein. In addition, the system further comprises a policy generator for generating the policy specification file (Inherent feature of a system having a policy specification file).

20. As per claim 12, the rejection of claim 1 under 35 USC 103(a) as being unpatentable over Gleichauf in view of Rogers is incorporated herein. Neither Gleichauf nor Rogers teach encrypting the network packet data received by the policy monitoring component. However, it is notoriously well-known in the art to encrypt network packet data to prevent interception and tampering of transmitted data. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made to encrypt the network packet data to ensure the integrity of the system as necessary for a system that performs security assessments. The aforementioned cover the limitations of claim 12.

21. As per claims 13-16, 18 and 20-24, they are method claims corresponding to claims 1-4, 6 and 8-12, and they do not teach or define above the information claimed in claims 1-4, 6 and 8-12.. Therefore, claims 13-16, 18 and 20-24 are rejected as being

unpatentable over Gleichauf in view of Rogers for the same reasons set forth in claims 1-4, 6 and 8-12.

22. As per claim 33, Gleichauf in view of Rogers cover a system as outlined above and further includes a system for developing a network security policy for a network, the system comprising:

g. means for creating an initial network security policy file (Rogers, fig. 3, reference no. 24);

h. means for ensuring the initial network security policy file is uploaded to a machine on the network (see Rogers, Figure 3, Reference No. 43);

i. means for running a network monitor on the machine to collect the network traffic (Gleichauf, col. 5:59-61);

j. means for the network monitor outputting the collected network traffic in an output file, and passing the output file to a policy monitor component of Claim 1 (Gleichauf, 5:7-8);

k. means for the policy monitor monitor analyzing the collected network traffic (Gleichauf, 5:60-6:67);

l. means for storing the analyzed network traffic in a database (Gleichauf, fig. 2, reference no. 36; figs. 5A-C; col. 7:22-27 and lines 57-62; 8:1-8);

m. means for examining the analyzed network traffic in the database by querying the database using a query tool (Gleichauf, col. 8:20-21).

23. Gleichauf does not expressly teach means for modifying the initial network security policy file as needed; until a comprehensive and desired policy file is attained; and means for repeating from the means for ensuring network security policy file is uploaded through the means for modifying the network security policy file until a comprehensive and desired policy file is attained. Rogers discloses repeatedly updating the system state due to changes to system attributes or conditions as a result of changes in the network system parameters being monitored, and/or due to changes in local variables caused by the results of actions or policies after completion or caused by changes reflected due to a submission of a action or policy (Rogers, 17:7-52). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the initial network security policy file as needed and repeating from the means for ensuring network security policy file is uploaded through the means for modifying the network security policy file until a comprehensive and desired policy file is attained, since it ensures a more secure system for developing a security policy by enabling a continuous adjustment to the security policy driven by real-time events. Rogers, 2:6-20. The aforementioned cover the limitations of claim 33.

24. As per claim 34, the rejection of claim 33 under 35 USC 103(a) as being unpatentable over Gleichauf in view of Rogers is incorporated herein. In addition, the network machine is remote. Furthermore, uploading a file to a remote network machine is a well-known step in the art (ex. ftp); hence, Gleichauf in view of Rogers further comprise means for uploading the modified network security policy file to the remote

network machine as needed (see also Gleichauf, col. 5:35-46; Rogers, Figure 3, Reference No. 43).

25. As per claim 35, the rejection of claim 33 under 35 USC 103(a) as being unpatentable over Gleichauf in view of Rogers is incorporated herein. In addition, the system further comprises means for monitoring network traffic by using the attained comprehensive and desired policy file (Gleichauf, 5:58-67; Rogers, Figure 3).

26. As per claim 36, the rejection of claim 35 under 35 USC 103(a) as being unpatentable over Gleichauf in view of Rogers is incorporated herein. In addition, means for monitoring traffic is on a continuous basis (Gleichauf, 5:58-63).

27. As per claim 37, the rejection of claim 33 under 35 USC 103(a) as being unpatentable over Gleichauf in view of Rogers is incorporated herein. In addition, the system further comprises means for generating reports from the database, and using the generated reports as input for further policy refinement and/or using the generated reports for continuously monitoring network traffic (Gleichauf, col. 6:53-67; 8:31-35).

28. As per claim 38, the rejection of claim 37 under 35 USC 103(a) as being unpatentable over Gleichauf in view of Rogers is incorporated herein. In addition, means for encrypting the reports and sending the encrypted reports to a remote Web

server is an obvious limitation. See claim 12 rejection. The aforementioned cover the limitations of claim 38.

29. As per claim 39, the rejection of claim 38 under 35 USC 103(a) as being unpatentable over Gleichauf in view of Rogers is incorporated herein.In addition, the system further comprises means for accessing the reports on the remote server in a user-friendly manner (Gleichauf, col. 7:22-26 and lines 38-40).

30. As per claim 40, the rejection of claim 33 under 35 USC 103(a) as being unpatentable over Gleichauf in view of Rogers is incorporated herein. In addition, the means for creating an initial network security policy file and the step of modifying the network security policy file as needed uses a policy generator tool (Rogers, 17:7-52).

31. As per claims 25-32, they are method claims corresponding to claims 33-40 and they do not teach or define above the information claimed in claims 33-40. Therefore, claims 25-32 are rejected as being unpatentable over Gleichauf in view of Rogers for the same reasons set forth in claims 33-40.

32. Claims 7 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf in view of Rogers, and further in view of Vaid et al. USPN 6,502,131 (hereinafter Vaid).

33. As per claim 7, the rejection of claim 1 under 35 USC 103(a) as being unpatentable over Gleichauf in view of Rogers is incorporated herein. Neither Gleichauf nor Rogers discloses the system further comprises a secure web server comprising a web server component and a report database for displaying reports online, the reports generated by the events database using a report script. Vaid discloses management means to implement policy-based schema for security and resource management on firewall platforms. The invention disclosed includes a graphical user interface to monitoring and profile traffic by an administrator (Vaid, col. 4:35-45; Figures 9-15). It is further notoriously well known in the art to provide graphical tools on the web via a web server. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the system to further comprise a secure web server comprising a web server component and a report database for displaying reports online, the reports generated by the events database using a report script. One would be motivated to do so for a more user friendly means of managing a network as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 7.

34. As per claim 19, it is a method claim corresponding to claim 7 and it does not teach or define above the information claimed in claim 7. Therefore, claim 19 is rejected as being unpatentable over Gleichauf in view of Rogers and Vaid for the same reasons set forth in claim 7.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

KAMBIZ ZAND
PRIMARY EXAMINER

May 5, 2006